ICS 43.040
CCS T 35

中华人民共和国国家标准化指导性技术文件

GB/Z XXXXX—XXXX

、

道路车辆 电子电气系统 ASIL 等级确定方法指南

Road vehicles-ASIL determination guidelines for electrical and electronic system

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

（本草案完成时间：2021 年 4 月 1 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会（SAC/TC114）归口。

本文件起草单位：

本文件主要起草人：

道路车辆 电子电气系统ASIL等级确定方法指南

1 范围

本指导性技术文件提出了确定道路车辆电子电气系统ASIL（汽车安全完整性等级）的方法。确定电子电气系统的汽车安全完整性等级（ASIL）是GB/T 34590.3-XXXX中所要求的。

本指导性技术文件适用于安装在除轻便摩托车外的量产道路车辆上的包含一个或多个电气/电子系统的与安全相关的系统。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 34590-XXXX(所有部分) 道路车辆 功能安全

3 术语和定义

GB/T 34590.1-XXXX界定的术语和定义适用于本文件。

4 危害分析和风险评估

4.1 危害的识别

危害分析和风险评估（HARA）是一个分析过程，即识别潜在的危害，并与运行场景进行组合，形成一组特定的危害事件，评估每个危害事件的风险以确定其ASIL等级和安全目标。

相关项定义是进行HARA的前提条件。危害识别可通过不同的危害分析技术实现。本文件给出了使用危害与可操作性分析（HAZOP）技术进行危害识别的示例。HAZOP是一种探索型的分析方法，可用于识别和评估相关项的功能异常表现，有助于结构化和系统地检查相关项在整车层面的运行情况，该分析方法通过给相关项的每个功能添加适当的引导词来假定其不同的功能异常表现，该功能异常表现可导致危害，而该危害可能对目标车辆的驾乘人员，其他车辆及其乘客，或其他处于风险中的人员，如目标车辆附近的行人、骑自行车的人员或维修人员造成潜在伤害。

其他有效的方法也可用于识别相关危害，本文件不推荐也不支持某种特定的危害识别方法，危害的识别是危害分析和风险评估的一部分。

下面是一个简单的HAZOP方法的应用示例，用于识别相关项潜在的功能异常表现所导致的危害。例如，基于在相关项定义中所描述的功能，考虑相关项执行器的作用和能力，进而假设如下的相关项功能异常表现：

a) 功能丧失——在有需求时，不提供功能；
b) 在有需求时，提供错误的功能：
   1) 错误的功能——多于预期；
   2) 错误的功能——少于预期；
   3) 错误的功能——方向相反。
c) 非预期的功能——在无需求时，提供功能；
d) 输出卡滞在固定值上——功能不能按照预期更新。

注1：相关项处于功能异常时，可考虑在进行与相关项的维修不相关的任务时对维护人员的伤害。然而，对已有故障、已损坏或已拆解的相关项进行维修时，危害分析和风险评估不考虑相关项的已有故障对维护人员的伤害。例如，电动助力转向系统有在转向助力振荡这个故障情况下关闭助力功能的安全机制。当进行此故障的维修

时，维修人员可强制开启助力功能以识别故障的原因。这种情况不能使用危害分析和风险评估方法进行分析，因为这是维修人员为了进行维修而故意操作的。

注2：根据GB/T 34590-XXXX，危害分析和风险评估基于相关项的功能异常表现。

注3：并非所有的HAZOP引导词[1]都适用于所有的分析，可根据分析的范围和内容对引导词进行剪裁。使用者可选取一组特殊的HAZOP引导词用于分析。

针对车辆的两种功能，即转向助力和制动控制，表1提供了使用HAZOP方法识别功能异常表现的示例。

表 1　HAZOP 方法应用示例

功能	引导词					
	功能丧失	在有需求时，提供错误的功能			非预期的功能（在无需求时，提供功能）	输出卡滞在固定值上（功能不能按照需求更新）
		错误的功能（多于预期）	错误的功能（少于预期）	错误的功能（方向相反）		
转向助力功能	助力丧失	助力过大	助力不足	助力反向	非预期助力	转向锁死（转向输出卡滞在固定值或固定位置）
制动控制功能（传统制动功能）	制动丧失	制动过大	制动不足	-	非预期制动	制动锁死（制动输出卡滞在固定值或固定位置）

注4：在相关项的安全概念设计或后续的确认过程中，宜考虑车辆不同功能之间的相互作用。例如：单独来看，相关项的功能丧失可作为一种降级模式，但考虑到相关项间的相互作用和依赖关系，在整车层面上可能不是安全状态。

一旦某项功能潜在的功能异常表现被识别出来，将继续开展危害分析活动，分析每个功能异常表现在整车层面上产生的危害。在此分析过程中，应考虑车辆的运行场景，包括相关项生命周期的各个阶段（如：运行、服务和报废阶段）。

同一个功能异常表现可能造成多个整车层面的危害，这取决于车辆在不同运行场景中的行为表现。例如，非预期或过大的制动可能引起车辆非预期的减速和非预期的侧向移动，这取决于驾驶场景。

另外，相关项的多个功能异常表现可能造成相同的整车层面危害。危害分析和风险评估是一个迭代过程。考虑到不同的车辆运行场景和相关项生命周期阶段，相关项的功能异常表现和相应的整车层面危害也会在危害分析和风险评估的过程中不断更新。

表2和表3给出了将表1中基于整车功能所识别出的功能异常表现映射到整车层面危害的示例。该映射随功能异常表现所考虑的驾驶场景不同而不同（例如：制动丧失会导致减速能力丧失，车辆溜坡等）。

表 2　将转向助力功能的功能异常表现映射到整车层面危害的示例

功能异常表现	整车层面的危害
非预期助力	非预期的车辆侧向运动/非预期横摆
助力过大	
助力反向	
转向锁死（转向输出卡滞在固定值或固定位置）	车辆侧向运动控制丧失
助力不足	转向沉重（手力矩增大）
助力丧失	

表 3　将制动控制功能的功能异常表现映射到整车层面危害的示例

功能异常表现	整车层面的危害
非预期制动	非预期的车辆减速
制动力过大	
制动锁死（制动输出卡滞在固定值或固定位置）	
制动丧失	非预期的车辆减速度降低
制动不足	
非预期制动	非预期的车辆侧向运动
制动力过大	
制动锁死（制动输出卡滞在固定值或固定位置）	

4.2　风险评估

在风险评估过程中，假设相关项的功能异常表现会引起某个危害。根据危害的定义，其作为伤害的潜在来源，极大依赖于功能异常发生时所处的驾驶场景。因此，第一步需要假设一种车辆驾驶或运行场景以用于定义伤害。基于该运行场景，根据本文件4.2.1中的指导确定该运行场景的暴露概率（E）。对于该危害事件，严重度（S）和可控性（C）分别由4.2.2和4.2.3的指导确定。对于一个给定的危害事件，基于合理可预见的包含相关项的车辆的运行场景，重复该过程。

风险评估的结果依赖于相关项、车辆和数据的可用性。相关项的功能的设计和车辆特征将影响导致伤害的场景的定义，以及E、S、C参数的等级和理由。分析人员应考虑这些因素，并以此为基础对所开发系统的特性进行分析。

对于每个已分析过的危害事件，应将最高ASIL等级及其分配暴露概率（E）、严重度（S）和可控性（C）的理由记录在案（例如，记录在危害分析和风险评估模板中）。

注1：确定暴露概率（E）、严重度（S）和可控性（C）的顺序可以调整（也就是重新排列）。本文件假定暴露概率（E）、严重度（S）和可控性（C）以图1的顺序确定。

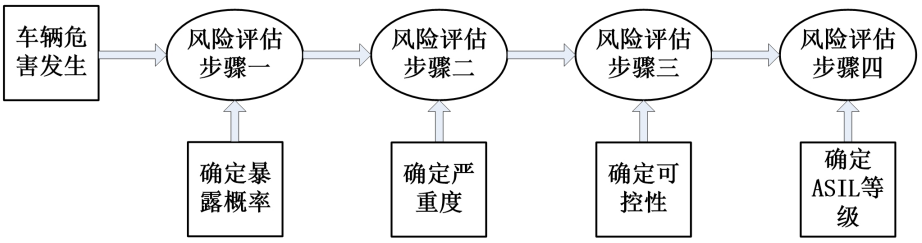


图 1　风险评估过程的示例

4.2.1　步骤 1：确定暴露概率

4.2.1.1　一般信息

根据GB/T 34590.3-XXXX,车辆运行场景的暴露概率可以被指定为表4中的五个等级之一。表4总结了GB/T 34590.3-XXXX中表2、附录B.2和附录B.3中的示例，得到基于运行场景频率和运行场景持续时间的各种暴露概率等级。按照图1，风险评估的第一步是针对特定的车辆运行场景评估暴露概率。特定的车辆运行场景可以是几个工况同时出现。确定暴露概率的目的是去理解真实场景，包括正常驾驶和危险驾驶工况。然而，需要注意的是不同的交通规则、环境条件等都会影响所考虑的场景，并可能由此导致不同的暴露概率。

表 4　GB/T 34590 中的暴露概率等级描述

等级	描述	基于频率的暴露概率的判定准则（参见GB/T 34590.3，表B.3）	基于持续时间的暴露概率的判定准则（参见GB/T 34590.3，表B.2）
E0[a]	不可能	未定义	无定义
E1	极低概率	对大多数驾驶员而言，一年发生的频率小于一次；	无定义
E2	低概率	对大多数驾驶员而言，每年发生几次	<1%的平均运行时间
E3	中等概率	对普通驾驶员而言，基本上每个月发生一次或多次	1%～10%的平均运行时间
E4	高概率	平均几乎发生在每次驾驶中	>10%的平均运行时间
[a] E0 无需分配 ASIL 等级。			

4.2.1.2　基于持续时间的暴露概率

对于功能异常表现直接导致危害事件的情况，可以选用基于车辆运行场景持续时间的暴露概率等级。

示例：考虑电助力转向系统使用了一个错误的转向扭矩。当车辆静止时，这对于驾驶员的影响可能很小，但如果车辆在高速路上行驶，则驾驶员很有可能偏离既定的行驶路线。由于车辆在该运行场景下的持续时间大于整体运行时间的10%，高速路行驶可以被定义为E4。

注：由危害导致潜在伤害的可能性会增加，这取决于涉险人员的行为或危害事件所处的环境。

4.2.1.3 基于频率的暴露概率

暴露概率等级不仅可以由功能异常表现直接引起危害事件（与场景的持续时间相关）的车辆运行场景确定，也可以由那些在某种场景或情况下，在更早的时间点出现并潜伏在系统中的故障所引起危害事件的场景确定。因此，这种场景的出现结合之前存在的故障会直接触发危害事件，而不需考虑其持续时间。

示例：对于车尾倒车灯激活的场景，可选择基于频率的方法来确定暴露概率。对于这个示例，可以认为“车辆倒车”的运行场景是经常发生的，所以选为 E4。选用频率是因为无论何时倒车灯出现故障，危害只可能在车辆挡位切换至倒车时才被触发。

4.2.1.4 车辆运行场景

图2给出了一系列车辆运行的场景作为参考。本示例清单不能认为是穷尽的，而且在很多情况下，这些场景可合并以减少或者简化在危害分析和风险评估中所考虑的场景（参考GB/T 34590.3-XXXX,6.4.2）。

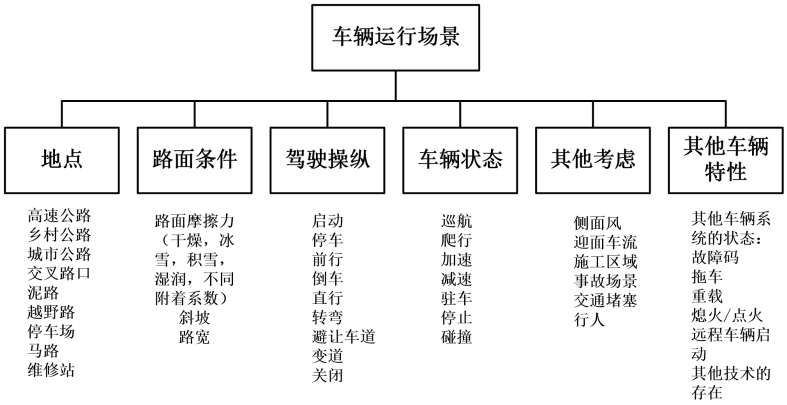


图 2 可能的车辆运行场景示例

4.2.1.5 暴露概率等级分配指南

a) 风险评估中的暴露概率分配，是根据对不同地理位置或目标市场的交通情况、文化、路况和驾驶方式的适用的且可用的数据和信息进行专家评估而得出的。当有疑问时，可以使用估计值。

b) 分配暴露概率时，可考虑暴露于车辆运行场景的频率,或暴露于该车辆运行场景的整体持续时间的概率。在某些情况下，两种暴露概率准则都可适用,此时,必须分别评估每个准则并指定各自的 ASIL。

示例：对于“洗车”场景的暴露概率，基于暴露的频率可以导出为 E3，而基于暴露的持续时间可以导出为 E2。

c) 通过考虑某一车辆在实际使用中发生的场景，可以对暴露概率进行评估。如果适用，可以考虑特定目标市场的暴露概率。然而这不应该被用于人为增加或减少暴露概率的因素。

d) GB/T 34590.3-XXXX 中提供的车辆运行场景的示例，可作为暴露概率分配的参考。

e) 在评估某些车辆的运行场景时，可能需要多种因素组合才能使危害导致特定伤害。某一车辆运行场景可能由几个因素构成，此外，这些因素中的某些因素可能会有密切的关联。针对形成危害事件的先决条件的因素组合，其暴露概率的正确值，需在识别各个因子的相互关系后才能计算出。

示例：对于有雪且有冰的场景，那么它们与路面摩擦力的降低有很高的相关性。如果有雪或有冰的场景的暴露概率对于道路摩擦力的降低被分别认为是彼此独立的 E2 等级，那么不应该用这两个定级为 E2 的暴露概率因子等效出一个低于 E2 的暴露概率（来针对有雪且有冰的场景）。错误地把这些因素视为独立的，的确会导致暴露概率的降级。

f) 在危害分析和风险评估时，不应该针对维修人员评估已经被工作场所的安全规章制度所覆盖的危害，以及正在被维修的相关项所引起的所有危害(参见 4.1，注 1)。

g) 已定义的危害事件必须足够具体，以保证准确地定义伤害程度和确定可控性。

——某个场景可划分为几个新增的特定场景(可能导致不同的 S、C 参数)；

——如果与相同危害相关的多个场景的分析结果相似或者相同，应将这些场景组合起来分析；

——不应使用以上指南人为地增加或减少暴露概率因素；

——这并非要求穷尽地检查每种可能的组合，考虑典型的车辆运行场景并包含了那些可以导出最高 ASIL 等级的场景就足够了。

4.2.2 步骤 2：确定严重度

4.2.2.1 4.2.2.1 一般信息

按照GB/T 34590，由于某个特定危害事件引起的潜在伤害的“严重度”等级，可被定义为表5所示四个级别中的一个。这些“严重度”等级是为某个给定危害事件分配ASIL等级提供指导的通用分类。

通常，“严重度”等级很难确切地被定义。因为，任何一次实际碰撞的“严重度”结果与许多因素相关，而这其中很多因素无法被提前确定。影响严重度的因素包括：

a) 碰撞的类型，比如平面碰撞（例如正面、尾部、侧面碰撞）；

b) 碰撞参与车辆间或单个车辆碰撞事故发生时（与被撞物体）的相对速度；

c) 碰撞相关车辆的相对大小、高度、以及结构完整度（即碰撞兼容性）；

d) 车内乘员以及车外有碰撞风险人员的健康和年龄情况；

e) 车内乘员对于安全保护装置的使用情况（例如：安全带、儿童安全座椅）；

f) 有资质的且迅速的紧急救援（紧急救援队）的可用性及响应。

这些因素中，可能可以预测一些碰撞特性以及在某些情况下估计碰撞的相对速度。大多数会影响某一假定危害事件所引起的伤害“严重度”的其他因素，无法被很合理地提前预测。上述因素可作为用于风险评估中确定暴露度和可控性的因素的一部分。

除了可被忽略的碰撞，几乎所有碰撞产生伤害包括致命伤害的可能性永远不会为零。对于所有道路使用人员（例如，行人和骑自行车人员）来说，影响伤害可能性的特性是极为不同的。涉及交通事故的人员可能是年轻健壮的人，他们可以承受较大的碰撞力而不会产生持续严重的伤害。也可能是年老体弱的人，他们即使发生较轻微、低速的碰撞也会产生较大的伤害。因此，几乎针对任何碰撞类型所引起的“严重度”结果，可能是从“几乎无伤害”到“致命”的分布组合。

表5提供了GB/T 34590.3-XXXX中对于S0-S3严重度等级的描述。

表 5 GB/T 34590-XXXX 对于 S0-S3 严重度等级的描述

严重度等级	描述
S0[a]	无伤害
S1	轻度和中度伤害
S2	严重的和危及生命的伤害（有存活的可能）
S3	危及生命的伤害（存活不确定），致命的伤害
注：可参考GB/T 34590.3-XXXX，表B1针对“严重度”等级分类的示例。	
[a] S0 无需分配 ASIL 等级。	

基于有代表性的危害场景，将“严重度”等级分配到给定的危害事件。对这个假定场景的开发要包含多个信息来源，包括但不局限于专家分析和判断，以及技术报告分析特别是相关事故或测试、仿真试验和历史事故数据的分析。附录B提供了一些可以用于对某个给定整车层面的运动控制危害分配恰当“严重度”等级的一般信息。

4.2.2.2 碰撞相关危害“严重度”分配指南

在危害分析和风险评估过程中，分配“严重度”等级需要专家评估并考虑有代表性的各种交通状况、车速和路况的样本。由于车道和车辆技术（碰撞防护和避免）的持续进步和对道路使用人员安全行为的教育和法律实施力度的加强，分析历史事故数据倾向于过高估计未来针对伤害风险的措施，也可能不包含为某个新的不同场景的合适的数据。在这些情况下，为更好地预测结果，可以利用模型在历史数据环境中加入新的场景。

一般来说，道路使用者的伤害风险会随着碰撞速度的增大而增加。对于平面碰撞，在某些历史事故数据库中可得到的碰撞前后速度差值（Δv）的估算可以辅助事故“严重度”的评估。可以考虑用其他碰撞前后的估算量替代Δv（例如，能量等效速度、车辆/物体间相对速度），并考虑其他碰撞特性，如车辆重叠和挤压/侵入。附录B提供了一些可以辅助于“严重度”评级的一般指导。对于非平面碰撞，例

如翻车，其他可用的取决于危害场景的准则可以用于“严重度”评估。GB/T 34590.3-XXXX中给出的示例也可以用作“严重度”分配的参考。

当通过历史数据确定碰撞产生的可能的“严重度”等级时，应该考虑与正在开发的系统相关的可用数据。例如，由于新的主动安全特性的引入，在某些特定碰撞迫近环境中，这些主动安全特性会自动干预车辆的动态控制，驾驶员与车辆控制间的平衡正在发生变化。因此，随着新功能的应用，目前的数据可能无法反映合适的结果。在确定“严重度”和ASIL等级时，车辆或系统制造商应该考虑所有被应用于特定车辆的技术。

被考虑的有代表性的各类场景下形成的危害事件的“严重度”等级要记录在危害分析与风险评估文档中。

注1：宜考虑“暴露概率”来设定与之相关的“严重度”等级。对某驾驶工况，如果选择了比该驾驶工况对应的交通数据显示的“严重度”等级更高的值，则在评估暴露概率时，宜选择与此高“严重度”相对应的工况以进行“暴露概率”评估。

注2：历史事故数据不一定能够预测未来事故类型的伤害结果。由于车辆、道路和道路使用者行为一直在朝着增强交通安全的方向变化，历史数据倾向于过高估计未来事故的风险和伤害严重性。因此，不推荐简单的应用历史事故数据来预测某一特定整车层面危害的伤害后果和“严重度”等级分配。

4.2.3 步骤 3：可控性的确定

4.2.3.1 一般信息

根据GB/T 34590.3-XXXX，危害事件的可控性为表6所示的四个等级之一。

表 6 按照 GB/T 34590-XXXX 可控性等级描述

可控性等级	描述	详细描述
C0[a]	可控	如果针对特定危害存在专用法规，当它在考虑控制的充分性上与现有的经验保持一致，可控性可以评C0。对于使用C0可以参考GB/T 34590.3-XXXX,6.4.3.9。
C1	简单可控	超过99%的普通驾驶员或交通参与者能够避免伤害
C2	一般控制	90%到99%普通驾驶员或交通参与者能够避免伤害
C3	难以控制或不可控	不到90%普通驾驶员或交通参与者能够避免伤害
注：“特定危害”见GB/T 34590.3-XXXX，7.4.3.7，注2。		
[a] C0 无需分配 ASIL 等级。		

4.2.3.2 可控性等级分配的指南

可控性等级可以通过使用现有的数据、通过在模拟器或车辆进行测试、或通过咨询跨学科专家团队（例如，人为因素）来确定，可控性等级的确定应基于目标市场情况（例如，交通参与者的控制能力，场景因素等）。

GB/T 34590.3-XXXX附录B提供了“可控性”的示例，可作为“可控性”等级分配的参考。

在确定可控性时，只要电气/电子系统故障可能引起驾驶员的反应，则应考虑危害对涉险人员的不利影响（参考GB/T 34590.3-XXXX，7.4.2.7）。为评估这种潜在的不利影响，可参考参考文献[2][3]的方法。

由于驾驶员自身损伤（即，使用药物、酒精或睡眠不足）或驾驶员注意力不集中或分散引起的延长响应时间不在可控性的考虑范围，见GB/T 34590.3-XXXX，6.4.3.8，注2。

合理可预见的误用如果适用于特定的分析，应予考虑。

相关的环境特征（例如道路护栏）和驾驶员经验/行为/培训可以考虑在内。相关的车载系统如果能够减轻危害事件中的危害，且相关项和车载系统之间存在足够的独立性，则可以在危害分析和风险评估中将其考虑在内。

如果安全系统或驾驶员辅助系统是选配（例如，车道保持辅助系统），则在为特定车辆平台设定可控性级别时，不应被视为降低风险的措施。

4.2.4 步骤 4：ASIL 的确定

4.2.4.1 结合 S、E、C 确定 ASIL

按照GB/T 34590.3-XXXX，6.4.3.10，使用与GB/T 34590.3-XXXX表4所一致的参数“严重度”、“暴露概率”和“可控性”确定每一危害事件的ASIL等级。ASIL等级的确定基于相关的场景，且在该场景下S、E和C是一致的。

注：如果一个新系统的ASIL结果与相似的已经存在的且有很长的市场历史的系统的危害经验不一致，那它可能表明用于为新系统导出S、E和C的市场和交通数据需要重新审视。这也与“危害分析和风险评估”过程在本质上是可以迭代的事实是一致的。

表 7 按照 GB/T 34590.3-XXXX 确定 ASIL 的准则

ASIL确定		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

当为一个新系统确定ASIL等级时，如果适用，则由于该新系统的功能异常表现而导致事故的发生及其严重度，可以与现有的相关事故数据做对比。然后可评估测试对象对危害的反应行为，以导出初步的可控性等级。

应避免高估严重度、暴露概率和可控性参数以及导出的ASIL等级，否则可能导致对于提升车辆整体安全性有益的功能或特性的减少，甚至取消。同样的，评价者也应该避免低估严重度、暴露概率、可控性参数以及导出的ASIL等级，否则可能导致安全要求的不足。

4.3 安全目标与安全状态的关系

在执行“危害分析和风险评估”时，输出的是一组安全目标以确保安全运行。这些安全目标的定义考虑避免或者减轻相关项的故障行为可导致的潜在危害，可控性度量可以用于安全目标的定义。在功能或技术安全概念中，适当地定义了安全状态和相关的安全措施，以在相关项故障时实现安全目标。并不总是要求对安全状态进行“危害分析和风险评估”，尽管当安全状态和相关项层面的特定失效一致时，安全状态的危害可以由“危害分析和风险评估”导出。因此，由于安全目标和安全状态均源于对安全生命周期中不同点的故障行为的考虑，可能会导致不一致。为了安全档案的一致性，建议让安全状态不违反安全目标。此建议可通过对安全目标和各安全状态的不同阐述来实现。例如，安全目标可为“避免在没有报警的情况下丢失紧急制动功能”而安全状态可为“禁用功能并通知驾驶员该功能是不可用”。在这种安全状态下，报警会减轻功能丧失的后果，因为驾驶员会意识到自己不能依靠它。 安全概念和HARA必须保持一致，否则会对安全档案产生不利影响。 如果此安全目标的安全状态导致违反了另一个不太重要的安全目标，则必须注意使其各自的安全要求保持一致。并建议提供支持该策略的理由。

示例：假设存在这样一个系统：该系统的安全目标是避免某个系统失效，且该安全目标的 ASIL 很高。然而，由于在以前的项目开发中，该系统失效被分配一个较低的 ASIL，因此，功能安全工程师在概念阶段开发过程中错误地将该系统失效定义成了一种“安全状态”。之后，在根据单点故障度量评估部件失效风险的硬件设计阶段，发现概念阶段定义的安全机制非但不能降低系统风险，反而会引起系统失效，该技术安全概念存在自相矛盾的地方。为了解决这个问题，需要重新定义“安全状态”，或者重新定义失效模式，同时重新进行危害分析和风险评估。

附 录 A
（资料性）
整车层面的运动

本附录简要讨论沿不同车辆轴线可能的整车层面的运动。图A.1展示了车辆的运动方向，共计6个自由度。其中三条直线箭头x、y、z分别代表纵向、侧向和垂直运动方向，而绕着这三个方向的旋转p、q、r分别是侧倾、俯仰、横摆。非预期的相关项行为可能会潜在影响车辆沿一个或多个轴的运动。

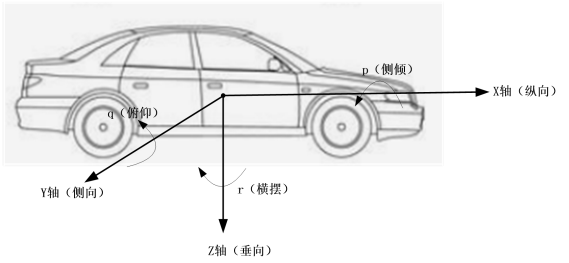


图 A.1 车辆运动轴

表A.1对于由于相关项功能异常潜在引起车辆沿坐标轴方向（或绕着车辆坐标轴方向）的运动，提供了系统性分析的指导。该表适用于“危害分析和风险评估”阶段，通过该表可以为相关项的每个潜在危害推导出对应的整车层面危害事件。

表 A.1 沿车辆各轴向的潜在危害行为示例

车辆运动	车辆潜在的危害行为
纵向运动（沿x轴）	非预期的加速
	非预期的加速能力丧失
	非预期的减速
	非预期的减速能力丧失
	非预期的纵向运动
	非预期的失去纵向运动控制
	非预期的反向运动
侧向运动（沿y轴）	非预期的侧向运动
	非预期的失去侧向运动控制
垂向运动（沿z轴）	非预期的垂向运动
俯仰（绕y轴旋转）	非预期旋转运动（绕y轴旋转）
侧倾（绕x轴旋转）	非预期旋转运动（绕x轴旋转）
横摆（绕z轴旋转）	非预期旋转运动（绕z轴旋转）
	非预期的失去旋转运动控制（绕z轴旋转）

附 录 B
（资料性）
严重度分级指南

B.1 总体介绍

本附录包含对车辆运动控制类危害分配严重度等级的总体信息，这类危害构成危害分析和风险评估的一部分。然而，本附录中的内容并非完全穷尽和确定，在应用中应予以注意。

严重度等级的分配可能涉及多种信息来源，包括（但不强制要求或限于）：专家分析和判断、分析特定相关碰撞或碰撞测试的技术报告、仿真测试或碰撞事故的历史数据。碰撞事故、实验室测试、道路测试及其它测试数据可提供客观、可信且可重复的结果。仿真测试可以为碰撞前的场景和碰撞事件中通常出现的许多因素和相互作用的相对贡献提供方向。对交通事故历史数据的分析可为各种碰撞事故情况提供事故发生频率和伤害可能性的总体指导。然而，固有的局限性使其无法对未来的经验作出精确的预测。

对基于车辆碰撞事故的场景，GB/T 34590.3-XXXX基于碰撞事故中人员受到的损伤，定义了严重度等级的概念（参见表B.1）。GB/T 34590.3-XXXX引用了简明损伤定级（AIS）（该等级对单一损伤分配了1-6的严重度评分），并将特定AIS等级的“损伤可能性”作为分配S0-S3严重度等级的例证。在一些历史事故数据库中提供了确定地理位置内的交通事故中涉及的部分或所有道路使用者所受伤害的AIS。这些事故数据的收集通常是小样本，案例选取准则因地点而异。

为恰当的使用来源于可用事故数据库的损伤评级，必须考虑数据来源的固有局限。使用事故数据来支持严重度分级时，要求对所收集的数据及可用数据的局限性有充分的理解，以确保采用了合适的方法、且结果得到了恰当的解释说明。

一般来说，文献刊物和真实世界中全球不同碰撞事故数据库的分析都揭示了碰撞事故严重度随相对速度的升高而增加的原理。为此，更高的行驶速度将可能增加在更高相对车速下碰撞事故的可能性，随之导致损伤可能性的升高。然而，基于不同的事故历史数据来源和特定撞车事故筛选准则来考虑为S0-S3的分配定义速度区间时，可能存在很宽泛的变化。这些变化也许是由于交通环境的区域性差异、事故历史数据抽样准则的变化、也可能是由于考虑了可用的碰撞事故属性、碰撞事故形式、配备或使用的乘员约束等其他因素。

为支持严重度分级，对于文献或特殊开发的分析中具备的历史事故数据的使用，技术上和实践上的考量包括：

——对于深度事故数据库，案例抽样准则和收集的数据在全球范围内有所不同。不同数据库的分析结果的差异可能部分归因于采样准则的变化。

——应考虑样本量的大小以更好地理解事故抽样过程中的不确定性，因为抽样过程随每个可用数据库而变化。特别是，在现有的深度事故数据库中，达到最高伤害严重度的碰撞事故所发生的低频率可能会限制得出任何损伤分级，进而限制支持严重度的分配。

——对感兴趣的人群的选择（分析层面）。对于一组给定的碰撞事故，基于记录的最高损伤严重度，对碰撞事故、对所涉及的车辆、对道路使用者以及对车辆使用者的损伤评级可能会有所不同。也就是说，对于任何一组特定的碰撞事故，在撞车事故层面、整车层面或乘员层面计算出的特定严重度损伤等级都是不同的。

——按照 GB/T 34590.3-XXXX，6.4.3.2 注 1，严重度分级宜考虑在事故中涉及的所有参与者可能遭受的损伤。

——碰撞事故后收集的可能与损伤风险有关的许多数据在撞车前是未知的，因此这些数据无法用于碰撞前的场景中。示例包括：乘员特性（例如：在类似的碰撞事故中，年长乘员一般来说会比年轻乘员受到更高的损伤风险）和碰撞对象特性（例如：大型商用车轻载与满载情况相比，碰撞能量潜能是不同的。）

——碰撞事故发生后对碰撞能量的预估（例如：相对车速、避障等效车速）：

- 不一定对每辆车进行计算（例如：在美国目前拖车碰撞事故案例中，如果碰撞对象是中型/重型卡车，无可用的相对速度预估）；
- 不一定与乘员碰撞脉冲一致，乘员碰撞脉冲可能受到特定碰撞特性、车辆结构和内饰、乘员几何尺寸、约束系统等的影响；

- 不一定与碰撞前的行驶车速一致，甚至也不接近。

如果本文件的使用者能接触到由特定危害的仿真、测试或其他严重度预估方法得出的特定数据或信息（例如：特定车辆的或与未来应用特别相关的数据/信息），那么可以使用这些数据/信息。此外，如果车辆上其他安全系统（即，危害分析和风险评估中分析考虑的系统以外的其他系统）的存在能减少潜在的伤害，则也可以作为特定严重度等级分配及相关可控性等级分配中的考虑因素。所以，本附录提供的一般指导目的是支持使用者理解问题的复杂性，并做出恰当的决策（需要更进一步的专家分析）。本文件不对作为危害分析和风险评估一部分的严重度分级的特定方法进行推荐或支持。

在GB/T 34590-XXXX中没有给出特定的、可实施指导的情况下，开展了对文献刊物和历史事故数据库（包含碰撞后重构相对车速和损伤AIS评级）的分析。表B.1考虑了以下信息：损毁面、受伤人员的最大简化损伤量表（MAIS）、冲击力的方向、碰撞对象、及对乘员约束的使用。

GB/T 34590.3-XXXX，附录B的“表B.1 严重度等级举例”中，阐述了评审损伤评级时的通用指导。基于不同分析和评审在碰撞发生后对相对车速的估计，下表B.1给出了车速范围总结。尽管损伤评级通常随着碰撞速度的增加而升高，对S0-S3分配的车速范围却受所考虑的数据来源和碰撞事故的影响而存在较大的范围变化。然而，这些分析的速度范围是基于碰撞发生后对相对车速的重构，也可为S0-S3的分配提供一些总的初始指导。但需要指出的是，使用表B.1并不作为本文件要求的一部分。

为了获得一组离散的范围，分析人员可以只选择一个数据来源，并应用适当的选取准则和严重度准则进行诠释。执行此过程后，分配严重度等级的速度范围不会重叠。

注：表B.1的数据来源为GIDAS等全球不同数据库，如参考文献[4][5][6]。表中的速度区间仅为参考值，具体开展分析需要结合目标市场的数据来源确定。

表 B.1 从全球事故数据库的各种分析中得出的最小和最大速度范围（Δv）

碰撞类型	范围	S0	S1	S2	S3
正碰	最小速度		> 4-10km/h, 及	> 20-50 km/h,及	> 40-65 km/h
	最大速度	< 4-10 km/h[a]	< 20-50 km/h	<= 40-65 km/h	
后碰	最小速度		> 4-10 km/h , 及	> 20-50 km/h,及	> 40-60 km/h
	最大速度	< 4-10 km/h[a]	< 20-50 km/h	<= 40-60 km/h	
侧碰	最小速度		> 2-10 km/h, 及	>= 8-30 km/h, 及	>16-40 km/h
	最大速度	< 2-3 km/h[a]	< 8-30 km/h	<16-40 km/h	
注：上述清单是非穷尽的。在确定危害事件的严重度分级时，宜考虑潜在风险的参与者。这包括行人、骑自行车的人和其他车辆上的乘客（无论车辆是否在公共道路上）。					
[a] 某些分析中未定义					

B.2 说明

表B.1基于全球的交通事故数据，为获得危害分析和风险评估中选定场景的特定结果，宜慎重挑选适当的过滤准则，同时考虑分析范围并基于危害的本质进行必要的调整。表B.1用到的分析应用了以下要素：

——用于分析的合适数量的选择（例如：事故数量、事故中车辆数量或事故相关人员的数量）。

——所考虑的多种因素，例如：碰撞类型、偏置大小、约束的使用、乘员的年龄。

——基于以下来源于GB/T 34590.3-XXXX中概念的严重度分级：

- S0：不能被定义为安全相关的损坏，例如：与路边设施的轻微碰撞（非S1、S2或S3）；
- S1：> 10%可能性是AIS1-6（且非S2或S3）；
- S2：> 10%可能性是AIS3-6（且非S3）；
- S3：> 10%可能性是AIS5-6。

使用不同来源的事故数据作为危害分析和风险评估中严重度分级基础，要注意以下几点：

——虽然事故是按照一种定义良好的方法进行抽样的，但与官方统计数据相比，有一些偏差，可以通过标准化和公布的加权方法加以补偿。

——利用已有的数据库来确定仍在研制中的汽车的事故严重度，需要考虑在此期间发生的主被动安全以及道路基础设施的改进。影响这种进展的一种可能的方法是只考虑最近的车型年或装有某些系统的汽车（如 ABS、ESC、安全气帘、行人保护）。

——给定的危害工况可能导致一系列可能的事故场景。分析人员宜避免那些仅能通过后验而无法在危害分析和风险评估中预测的详细分析。

基于上述数据源的每个单独的分析，为严重度等级S0-S3生成了一组离散的速度范围。表B.1展示了独立分析的汇总结果，为严重度等级S0-S3中的每一个等级定义最小速度范围和最大速度范围。表B.1中展示的那些范围反映了不同分析产生的离散速度范围的重叠,这可能是由于可用数据源及分析方法的差异。这些差异可能包括：

——区域行驶模式和环境；

——深度事故数据库的碰撞选择准则；

——从深度事故数据库外推到更广泛的人群；

——区域车辆队伍组成；

——车辆选择准则（例如，车龄，特定车辆技术的装备，如安全气囊）；

——碰撞类型的定义-正、侧、后（例如，损坏的平面、冲击力的方向）；

——碰撞类型的分类（例如，重叠量）；

——包含的碰撞对象及分类；

——乘员包容（例如，座椅位置、约束使用）；

——乘员特性（例如，年龄）；

——包含的非乘员伤害结果（例如，行人、其他车辆上的乘员）。

建议使用者确保数据来源和解释适用于正在分析的危害事件。

附 录 C
（资料性）
转向功能危害分析和风险评估示例

C.1 总则

本附录提供了电动助力转向（EPS）辅助功能的危害分析和风险评估示例。C.3提供了HAZOP分析，以识别对应整车层面危害的EPS功能异常表现。C.4提供了一些EPS功能异常、导致的整车层面危害及相关ASIL等级的示例。必须指出的是，本附录不代表转向功能完整的危害分析和风险评估，而是针对EPS功能的功能安全危害的一个子集，以提供指导。

注：本资料性附录包含了所选危害事件的ASIL等级示例。ASIL等级的确定，由相关方协商确定。GB 17675-2021附录B给出了针对转向系统的最低要求。

C.2 相关项定义：功能概念概述

EPS功能辅助驾驶员为转向轮提供车辆方向控制，同时降低驾驶员进行车辆转向所需的操作力。EPS测量转向盘处的驾驶员意图，与车辆其他输入同时处理，以提供转向扭矩辅助。本分析的范围是，假设EPS系统具有机械转向连接，当EPS助力功能丧失时，仍能支持驾驶员人力转动车辆。

C.3 HAZOP 分析

表C.1展示了HAZOP分析以识别EPS助力功能的功能异常表现。表C.2展示了从EPS功能异常到车辆危害的映射。

表 C.1 电动转向助力功能的 HAZOP 分析

功能	引导词					
	功能丧失	在有需求时，提供错误的功能			非预期的功能（在无需求时，提供功能）	输出卡滞在固定值上（功能不能按照需求更新）
		错误的功能（多于预期）	错误的功能（少于预期）	错误的功能（方向相反）		
转向助力功能	助力丧失	助力过大	助力不足	助力反向（提供相对于请求的相反方向的助力）	非预期助力	转向锁止（转向输出卡滞在固定值或固定位置）

表 C.2 将转向助力功能的功能异常表现映射到整车层面危害的示例

功能异常表现	整车层面的危害
转向助力丧失	转向沉重（手力矩增大）
转向助力不足	
转向助力过大	非预期的侧向运动/非预期的横摆
反向转向助力	
非预期的转向助力	
转向锁止	车辆侧向运动控制丧失

C.4 危害分析和风险评估

表C.3显示了EPS助力功能相关HARA的部分示例。本附录中提供的HARA示例包含了与转向助力功能相关的车辆运动控制危害的示例，这些危害与功能安全相关。

表 C.3 电动助力转向功能的 HARA 分析示例

危害编号	功能	功能异常表现	整车层面的危害	假设	危害的详细描述	潜在的事故场景－考虑最严苛场景	ASIL（汽车安全完整性等级）的评估							备注
							S	理由	E	理由	C	理由	ASIL	
转向危害#1	转向助力	非预期的转向助力	非预期的侧向运动 / 非预期的横摆	无	当没有驾驶员要求时，转向系统非预期的提供扭矩动作。	在驾驶员能够控制之前，车辆会离开预期路径/车道并与迎面而来的或邻近的交通参与者或路边物体产生碰撞。如果转向产生非预期的横摆力矩，可能导致车辆失控。	3	高速公路上的高速车辆碰撞或与物体的碰撞	4	每天都暴露在城市道路或高速公路上	3	大多数驾驶员都无法控制这种情况	D	这种危害适用于转向扭矩或转向角度控制功能。ASIL可根据车辆和标定以及控制扰动的大小而降低
		反向转向助力			转向系统提供与驾驶员要求相反的方向上的扭矩动作。									
转向危害#2	转向助力	转向助力过大	非预期的侧向运动 / 非预期的横摆	无	转向系统提供比设计意图多的转向助力；感觉转向系统比正常轻，但响应方向与驾驶员要求相同。	在高速公路上高速行驶的车辆在变道期间，增加的助力可能导致驾驶员的过度转向。在驾驶员能够控制之前，车辆会离开预期路径/车道并与迎面而来的或邻近的交通参与者或路边物体产生碰撞。	3	高速公路上的高速车辆碰撞或与物体的碰撞	4	每天都暴露在城市道路或高速公路上	1	简单可控	B	这种危害仅适用于转向助力控制功能。 ASIL可根据车辆和校准值以及控制扰动的大小而降低。
转向危害#3	转向助力	转向锁止	非预期失去侧向运动控制	转向系统中有电阻	转向系统在电气上锁死或卡滞在某个特定位置，并且当车辆移动时不响应驾驶员请求。此类功能异常表现导致无法实现手动转向。	车辆按照转向系统和车轮的最后位置继续运动。驾驶员不能进行车辆转向。在驾驶员能够控制之前，车辆会离开预期路径/车道并与迎面而来的或邻近的交通参与者或路边物体产生碰撞。	3	高速公路上的高速车辆碰撞或与物体的碰撞	4	每天都暴露在城市道路或高速公路上	3	大多数驾驶员都无法控制这种情况	D	这种危害适用于转向扭矩或转向角度控制功能。
转向危害#4	转向助力	失去转向助力	转向沉重（手力矩增大）	具备机械转向连接; 转向系统符合GB 17675	当车辆行驶时，转向助力突然丢失。根据车辆和转向系统的顺应性，可能需要增加驾驶员手动转向力。	当车辆以较高的速度行驶时，只需要较小的转向助力来控制车辆方向。低速行驶时，及时施加足够地转向力对有些驾驶员可能是挑战。潜在地导致与交通中的车辆或行人发生碰撞。	S、E、C评级根据车辆不同而不同。对于突然失去转向助力，其ASIL等级取决于车辆设计和配置。以下是严重度、暴露概率和可控性分级的几个准则： 严重度可基于： ———车辆碰撞速度； ———与车辆/路边物体/行人的潜在碰撞； ———本标准附录 B 严重度表 B.1。							

危害编	功能	功能异常	整车层面的危	假设	危害的详细描述	潜在的事故场景－考虑最严苛场	ASIL（汽车安全完整性等级）的评估	备注
							暴露概率可基于： ———在特定车辆速度范围内在不同侧向加速度下的持续时间； ———暴露在威胁下的可能性。 助力丧失时的可控性可取决于与转向系统设计和车辆特性有关的多个因素，包括： ———可控性的重要度量之一是方向盘轮辋力； **注1：**基于GB 17675（基于EPS系统完整功能的转向力值）和MIL STD 1472，150 N被推荐为针对C1上限的指标。 **注2：**其他注意事项： ———当前市场上无转向助力行为的转向系统可能是可接受的； ———市场上无助力行为的转向系统可被用作未来系统设计准则的基准； ———在全球范围内，对于转向系统，符合 ECE-R79 是行业惯例。在中国，需符合强制性国家标准 GB 17675。	
注：危害分析和风险评估后，需要针对各个危害定义安全目标，安全目标的定义可以考虑代表目标市场人员对风险控制能力的可控性度量结果。								

附 录 D
（资料性）
驱动和传动功能危害分析和风险评估示例

D.1 总则

按照GB/T 34590-XXXX，针对与驱动和传动功能相关的功能异常表现和车辆层面危害，本附录给出危害分析和风险评估（HARA）的示例、指南和论据来确定汽车安全完整性等级（ASIL）。

必须指出的是，本附录并不代表一个完整的、针对驱动和传动功能的危害分析和风险评估，而是一个重要的、有意义的评估示例子集。这些示例不必为任何特定车辆系统定义最小或最大的汽车安全完整性等级（ASIL）。本附录仅提供示例，其中有足够的有效数据或明确的专家共识可用于允许形成一个共同的评估，并证明是有指导意义的示例。在实际的危害分析和风险评估中，需要对额外的场景进行评估以找到给出最高功能安全等级的场景。

注：本资料性附录包含了所选危害事件的ASIL等级示例。ASIL等级的确定，由相关方协商确定。。

D.2 相关项定义：功能概念概述

本标准的目的是给出一般性推荐而不是系统的具体评估，相关项定义必须尽可能保持通用。因此，只列出基本的驱动和传动功能，并且只有当这些功能被证明与示例风险评估相关时，标准中才会增加额外内容加以说明。表D.1提供关于驱动和传动系统基本功能的概述。

注：在使用所提供的示例时，需要注意某些参数是与车辆/系统强相关的，并且这些参数可以导致对不同车辆的风险评估结果的不同。必须在特定的HARA中考虑这些参数，以保证合理的结果。

表 D.1 功能列表

功能	详述和备注
提供动力总成启停选择	提供动力总成启停选择可表示为： ——传统发动机启停； ——电机启停； ——带有蠕行模式的启停； ——不带蠕行模式的启停； ——钥匙启动的启停； ——自动起停系统的启停； ——其它原因的启停（例如自动冷却/加热）。
提供可选的驾驶方向	提供可选的驾驶方向可表示为： ——前进（D）； ——倒退（R）； ——空档（N）。 **注：**基本功能是“车辆移动”（向前移动/向后移动/不移动）。 自动变速箱或线控换挡系统来提供驾驶方向。
提供所需驱动扭矩	提供所需驱动扭矩： ——通过传统动力总成； ——通过电动的动力总成； ——通过混合动力总成。
提供制动扭矩	提供制动扭矩： ——通过（电的）回收； ——通过（传统的）拖曳扭矩； ——通过自动变速箱装置。 **注1：**关于自动变速箱装置，可能需要区分不同的模式（例如：自动模式、运动模式、经济模式等）。 关于制动能量回收，有两种不同的方式： 1）与主制动无关的制动能量回收： 释放油门踏板，由高于常规的拖曳扭矩产生的制动能量回收(与车辆相关)； 2）与行车制动相关的制动能量回收： 踩下制动踏板后产生的制动能量回收（与制动系统的减速过程相结合）。

功能	详述和备注
	注2：方式（2）不在本附录的范围。
提供可选的/自动的防溜坡	提供可选择的/自动防溜坡： ——通过自动驻车(Auto-P) ——通过手动驻车(P) 功能也应该包含自动解锁和手动解锁 **注**：一个电气/电子相关系统被考虑用于防溜坡。

D.3 危害与可操作性分析

对于每一个被分析的功能，可以从潜在的非预期系统状态得出相关的整车层面危害。表D.2给出了概览。最后一列表明，某一功能异常是否与另一功能异常导致同样的风险评估结果。在此情况下，本附录未提供额外的功能异常示例。

表 D.2 危害与可操作性分析（HAZOP）结果以及功能、功能异常表现和潜在车辆层面危害的映射

危害编号	功能	功能异常表现	潜在的整车层面危害	与…相同
F1	基本功能：提供动力总成启/停选项			
F1-1	激活/关闭动力总成	非预期的激活动力总成	非预期的加速（蠕行）	
F1-2	激活/关闭动力总成	非预期的关闭动力总成	加速能力丧失（滑行）	
F1-3	激活/关闭动力总成	动力总成无法激活	无	
F2	基本功能：提供可选择的行驶方向			
F2-1	按预期方向移动	按非预期方向移动	按不正确的方向运动	
F2-2	按预期方向移动	不能移动	无	
F2-3a	挂“空档”	非预期的挂”前进/倒车档”,而不是”空档”	非预期的加速（蠕行）	F1-1
F2-3b	挂“空档”	非预期的挂“驻车档”,而不是“空档”	纵向运动丧失（低速）	F2-4b
F2-4a	挂“空档”	非预期的挂”前进/倒车档”，当车辆在“空档”时	非预期的加速（蠕行）	F1-1
F2-4b	挂“空档”	非预期的挂”驻车档”，当车辆在“空档”时	纵向运动丧失（低速）	
F3	基本功能：提供需求的驱动扭矩			
F3-1a	提供需求的驱动扭矩	提供的驱动扭矩大于需求	非预期的加速（车辆未失稳）	
F3-1b	提供需求的驱动扭矩	提供的驱动扭矩大于需求	非预期的旋转运动（沿垂向）--> 横摆	
F3-2	提供需求的驱动扭矩	提供的驱动扭矩小于需求	加速能力丧失（滑行）	
F4	基本功能：提供制动扭矩			
F4-1a	提供制动扭矩	提供的制动扭矩大于需求	非预期的减速（车辆未失稳）	
F4-1b	提供制动扭矩	提供的制动扭矩大于需求	非预期的旋转运动（沿垂向）--> 横摆	
F4-2	提供制动扭矩	非预期的缺少再生制动减速 (油门踏板释放时)	减速能力丧失	
F4-3	提供制动扭矩	非预期的缺少拖曳扭矩	减速能力丧失	
F5	基本功能：提供防溜坡功能			
F5-1a	提供防溜坡功能	非预期的防溜坡功能启动(车辆静止时)	纵向运动丧失(轴向锁定)	F2-4b
F5-1b	提供防溜坡功能	非预期的防溜坡功能启动（车辆行驶时）	纵向运动丧失(轴向锁定)	
F5-1c	提供防溜坡功能	非预期的防溜坡功能启动（车辆行驶时）	非预期的旋转运动（沿垂向）--> 横摆	
F5-2	提供防溜坡功能	非预期的防溜坡功能关闭	非预期的纵向运动	
F5-3	提供防溜坡功能	无法提供防溜坡功能	非预期的纵向运动	

D.4 危害分析和风险评估

D.4.1 整车运行场景/危害场景

对于本附录，仅分析一些最重要的运行场景作为每个危害进行风险评估的示例。每个场景都应能与特定的功能异常相结合，来进行特定危害场景的系统评估。

D.4.2 示例的选择

每个故障和危害事件都需要进行详细的讨论，并进行清晰的评估。所有可获得的结果（特定故障的最高ASIL等级）都从相关组织的已执行的危害分析和风险评估中收集到。如果所有的HARA分析的结果都是相同的，在本附录中只列举一个危害事件进行风险评估的描述性示例，以说明共同的结果。如果不同的HARA分析的结果各不相同，则应运用不同的示例及更详细的说明来解释产生不同结果的原因。具体示例见表D.3。

注：这些示例不能被理解成所有危害的穷尽清单。其它可能的功能丧失或者相关的整车层面危害应针对实际的相关项进行具体的危害分析和风险评估。

表 D.3 驱动和传动功能的 HARA 分析示例

危害编号	功能	功能异常表现	整车层面的危害	假设	危害的详细描述	潜在的事故场景－考虑最严苛场景	ASIL（汽车安全完整性等级）的评估							备注
							S	理由	E	理由	C	理由	ASIL	
F1	基本功能：提供动力总成启 / 停选项													
F1-3	激活/关闭动力总成	动力总成无法激活	--	无	车辆处于静止状态，同时动力系统停止，驾驶员想启动车辆。	车辆保持静止状态，没有危害影响	S0	车辆保持静止状态，没有危害影响	E4	--	--		QM	
F2	基本功能：提供可选择的行驶方向													
F2-2	按预期方向移动	不能移动	--	应单独分析置于空档下的非预期移动。		车辆将保持静止状态，没有危害影响。	S0	车辆保持静止状态，没有危害影响。	E4	--	--		QM	
F2-4b	挂“空档”	非预期的挂”前进/倒车档”，当车辆在“空档”时	纵向运动丧失（低速）	当车辆从前进档转换到停车档，需分开讨论。（参考F5-1）	车辆在洗车房	车辆和洗车场会被损坏。	S0	非预期的转到P档导致传动轴抱死。车辆和洗车场被损坏，没有人员伤害。	E2	车辆在洗车处。（E2，参考GB/T 34590.3-2017）	--		QM	当车辆处于空档时，一定时间后激活停车档可能是系统功能。
F3	基本功能：提供需要的驱动扭矩													
F3-1a (1)	提供需求的驱动扭矩	提供的驱动扭矩大于需求	非预期的加速（车辆未失稳）	对具有典型的驱动扭矩的车辆评估是有效的。 对于带较大扭矩力的高性能驱动系统，要综合考虑距离、碰撞速度、反应时间来决定评估为较高的ASIL等级是否更合适。（参考D.5.3的示例） 此外，失稳的风险也应被评估。（参考	车辆在城市或乡村道路上，跟随其它车辆后面。	车辆前部和其它车辆前部/后部碰撞	S2	车辆前部与另一辆车的后部以中等速度发生碰撞。（例如，车辆间相对速度20公里每小时）	E4	在车前部有其它车辆是很常见的现象。这被判断为超过10%的运行时间。	C2	这种情况可通过踩制动踏板来控制（驾驶员的直觉反应），对大多数情况，反应时间足够有效避免特定危害。	B	

危害	功能	功能异常	整车层面	假设	危害的详细描	潜在的事故场景	ASIL（汽车安全完整性等级）的评估							备注
				F3-1b的示例）										
F3-1a (2)	提供需求的驱动扭矩	提供的驱动扭矩大于需求	非预期的加速（车辆未失稳）		车辆低速行驶（例如，车辆处于一档），行人处于危险区域。	以一定的速度和行人正面碰撞（假设没有碾压）。	S2	碰撞速度相对较慢，因为初始速度很慢，并且行人被认为靠近车辆。	E3	在驾驶周期，周围有行人的情况（例如：交叉路口，停车场）占很高的比例。然而，据评估，仅一定比例的驾驶时间车辆处于这类位置，并且行人不总是处于危险区域。	C3	一些驾驶员会被车辆非预期的加速以及加速产生的车辆和行人的瞬间靠近惊吓，导致延长了反应时间。少于90%的驾驶员或所有交通参与人通常能够或勉强可以避免危害。	B	
F3-1a (3)	提供需求的驱动扭矩	提供的驱动扭矩大于需求	非预期的加速（车辆未失稳）	无	车辆低速行驶（例如，车辆处于一档）在行人易受伤害的区域或者碾压的情况发生。 这些情况取决于行人，但也取决于专门的车辆设计，（参考D.5.3）	正面和行人碰撞并碾压。	S3	该情况聚焦于事故场景，预期到碾压严重度评估为S3	E2 或E3	在驾驶周期，周围有行人的情况（例如：交叉路口，停车场）占很高的比例。然而，据评估，仅一定比例的驾驶时间车辆处于这类位置，并且行人不总是处于危险区域。 因为聚焦于碾压场景，可能性降低到一定程度。然而，还没有确定存在的数据对所有车辆决定暴露概率等级的通用结果。	C3	一些驾驶员会被车辆非预期的加速以及加速产生的车辆和行人的瞬间靠近惊吓，导致延长了反应时间。少于90%的驾驶员或所有交通参与人通常能够或勉强可以避免危害	B 或者C	
F3-1b	提供需求的驱动扭矩	提供的驱动扭矩大于需求	非预期的横摆角速度变化/非预期的旋转运动（沿垂向）	系统最高的ASIL等级取决于在特定驾驶场景下由于故障导致潜在的车辆失稳。这通常取决于系统特性，例如： a）非预期扭矩的大小(N.m)与坡度	对于评估，宜分析有关场景，系统性的选择最相关的参数： -路面摩擦力； -车辆速度； -转弯速度。	和路边物体或迎面车辆发生正面/侧面碰撞。	S2或S3	如果车辆失去抓地力并且驾驶员不能阻止非预期的横摆角速度变化： a) 前驱车辆将向前滑动（转向不足），但可能以一定速度偏离路面并和路边物体	E2 ~E4	对ASIL评级最重要的场景是车辆行驶在典型的乡村道路速度并具有中度侧向加速度。现在取决于在下列情况下系统特性是否稳定： a）干燥路面（E4）； b）潮湿路面（E3）；或 c）仅冰雪路面 （E2）。	C2	驾驶员第一应急反应是踩制动踏板。其次他可能切换到空档或关闭发动机。	QM ~C	ASIL等级和车辆、系统特性高度相关

危害	功能	功能异常	整车层面	假设	危害的详细描	潜在的事故场景	ASIL（汽车安全完整性等级）的评估							备注
				(N.m/s)； b）动力总成概念（前驱/后驱）、整车质量、负载分配等。				（例如：树）碰撞。 b）后驱车辆会很快过转向。可能与迎面车辆或路边物体发生侧面碰撞。		对于传统车辆，典型的扭矩水平和动态，最高为E3。对电动车辆则不同。 **注：**较高车速、较高侧向加速可能会降低E等级。				
F3-2	提供需求的驱动扭矩	提供的驱动扭矩小于需求	加速能力丧失（滑行）	需要注意，如果驾驶场景是几乎在稳定的极限，突然失去扭矩会导致失稳（由于纵向力的改变，侧向力也会被影响）。参考F4-1。	车辆在乡村道路超车，迎面有对开车辆。	与对开车辆发生正面碰撞	S3	如果不能按照预期快速完成超车，可能和对开车辆发生正面碰撞。在这情况下，伤害严重程度和车速高度相关。	E2	基于持续时间的评估：在有对开车辆时超车，是一种短时机动行为且发生机会不多，一般不超过1% 的运行时间。	C1	有对开车辆时超车需要驾驶员更注意和集中精力。他/她可以减速或踩制动踏板并回到原来车道。此外，对开车辆驾驶员可以减速、执行避让措施。	QM	
F4	基本功能：提供制动扭矩													
F4-1a	提供制动扭矩	提供的制动扭矩大于需求	非预期的减速（车辆未失稳）	系统最高的ASIL等级取决于坡度以及由故障引起的非预期减速程度			此类危害包含在附录F,具体参见F.4.1（制动危害1）							
F4-1b (1)	提供制动扭矩	提供的制动扭矩大于需求（后驱）	非预期的横摆角速度变化/非预期的旋转运动（沿垂向）	系统最高的ASIL等级取决于在特定驾驶场景下由于故障导致潜在的车辆失稳。这通常取决于系统特性，例如： a）非预期扭矩的大小(N.m)与坡度(N.m/s)； b）动力总成概念（前驱/后驱）、整车质量、负载分配等。	对于评估，宜分析有关场景，系统性的选择最相关的参数： -路面摩擦力； -车辆速度； -转弯速度。	和路边物体或迎面物体发生正面/侧面碰撞。	S3	如果车辆失去地面附着力并且驾驶员不能阻止非预期的横摆角速度变化， 后驱车辆会很快过转向。在没有提前减速很多时与对开车辆或路边物体发生侧面碰撞。	E2~E4	对ASIL评级最重要的场景是车辆以中等速度（例如：130 km/h）行驶并只有有限的侧向加速度(例如: 2 m/s²)。现在取决于在下列情况下系统特性是否稳定： a）干燥路面（E4）； b）潮湿路面（E3）；或 c）仅冰雪路面 （E2）。 **注：**较高车速、较高侧向加速可能会降低E等级。	C3	当车辆在潮湿或冰雪路面失去地面附着力和失去稳定时，驾驶员将不能重新控制车辆。对开车辆可能做出反应并减速。但是，对路边物体的碰撞很难控制。	B～D	ASIL等级和车辆，系统特性高度相关
F4-1b (2)	提供制动扭矩	提供的制动扭矩大	非预期的横摆角速	系统最高的ASIL等级取决于在特定驾驶场	对于评估，宜分析有关场	与路边物体或对开车辆的正面/	S2或	如果车辆失去地面附着力并且驾驶员不能	E2～E4	对ASIL评级最重要的场景是车辆以中等速度（例如：	C3	当车辆在潮湿或冰雪路面失	B 或C	ASIL等级与车辆和

危害	功能	功能异常	整车层面	假设	危害的详细描	潜在的事故场景	ASIL（汽车安全完整性等级）的评估						备注
		于需求（前驱）	度变化/非预期的旋转运动（沿垂直）	景下由于故障导致潜在的车辆失稳。这通常取决于系统特性，例如： a）非预期扭矩的大小(N.m)与坡度(N.m/s)； b）动力总成概念（前驱/后驱）、整车质量、负载分配等。	景，系统性的选择最相关的参数： -路面摩擦力； -车辆速度； -转弯速度。	侧面碰撞。	S3	阻止非预期的横摆角速度变化，前驱车辆将继续直行前进（在转向的情况下）。 在干燥道路上，车辆将迅速减速，但可能会以一定速度离开道路，并与路边物体如树等碰撞（S2）。 在湿滑或结冰道路上，车速未有效降低的碰撞是可能的，（S3）。		130 km/h）行驶并只有有限的侧向加速度（例如：2 m/s²）。现在取决于在下列情况下系统特性是否稳定： a）干燥路面（E4）； b）潮湿路面（E3）；或 c）仅冰雪路面 （E2）。 **注：**较高车速、较高侧向加速可能会降低E等级。 E4场景导致S2，E2/E3场景也可导致S3		去地面附着力和失去稳定时，驾驶员将不能重新控制车辆。对开车辆可能做出反应并减速。但是，对路边物体的碰撞很难控制。		系统特性高度相关。
F4-2	提供制动扭矩	缺少再生制动扭矩(油门踏板释放时)	再生制动减速能力丧失	类似“非需求的车辆滑行”	车辆低速行驶到人行横道，驾驶员期望通过再生制动减速度来停止车辆。	与行人低速碰撞	--	与行人低速碰撞	--	车辆低速行驶到人行横道，驾驶员想通过再生制动减速度来停止车辆。	C0	可认为对所有人都是可控的（C0），至少只要驾驶员所预期的再生制动减速度不太高（例如，< 3 m/s^2）	QM	
F4-3	提供制动扭矩	拖曳扭矩不足	拖曳减速能力丧失	类似“非需求的车辆滑行”	车辆低速行驶到人行横道时。驾驶员想通过拖曳扭矩减速度停止车辆。	与行人低速碰撞	--	与行人低速碰撞	--	车辆低速行驶到人行横道，驾驶员想通过拖曳扭矩减速度来停止车辆。	C0	可认为对所有人都是可控的（C0），只要制动系统是工作的。	QM	具有重型拖车的车辆在下坡时可能需要拖曳扭矩，以避免制动系统过热。
F5	基本功能：提供可选/自动的防溜坡功能。													
F5-1b	提供防溜坡功能	非预期的防溜坡功能启动(车辆行驶时)	非预期的减速	独立于系统的评估（“一般的防溜坡功能”） ->参见F4-1a										
F5-1c	提供防	非预期的	非预期的	独立于系统的评估										

危害	功能	功能异常	整车层面	假设	危害的详细描	潜在的事故场景	ASIL（汽车安全完整性等级）的评估								备注
	溜坡功能	防溜坡功能启动（车辆行驶时）	横摆角速度变化/非预期的旋转运动（垂向）	（“一般的防溜坡功能”） ->参见F4-1b											
F5-1d	提供防溜坡功能	非预期的防溜坡功能启动（车辆行驶时）	纵向运动丧失（极低速度）	特殊情况：典型的停车锁止系统。最大扭矩取决于停车锁止机构，因为它会在一定强度下损坏。 假定当驱动轴具有一定的最小速度时，存在防止停车锁止被啮合的机械措施。 在这种情况下，仅当速度非常低或驱动轴由于车轮阻挡而停止时（例如，在低摩擦路上进行没有ABS的制动）才可能发生故障。	车辆低速行驶（<5 km/h）到十字路口并且故障发生时。其他车辆从侧面驶来。	侧面与其他车辆的前端碰撞。	S2	侧面来车的最终影响在25 km/h ≤ Δv≤ 35 km/h 的范围内	E2	相关情况低于总运行时间的1%，例如当车辆合并到道路的内道时、横穿通行道路或转向拥有优先通行权的车道。	C2	驾驶员可以避免将车辆暴露于碰撞的风险。通过正确驾驶，将有足够的时间让侧面来车进行制动。	QM	参考D.5.1
F5-2 / F5-3	提供防溜坡功能	非预期的防溜坡功能关闭，或无法提供防溜坡功能	非预期的纵向运动	基于以下系统基本特性评估： （1）只有当电子电气系统处于激活时才可能有的故障。对于插电式电动车辆，相较于传统车辆，激活时间将更长； （2）当自动驻车制动可用时，驾驶员预期是不同的。	车辆停在有足够溜坡距离的斜坡上（发动机熄火）。（能达到危险车速）。行人或其他道路使用者处于危险区域（下坡）。	与行人或其他道路使用者碰撞。	--	严重度可从主要取决于距离和坡度的碰撞速度得出。	--	在斜坡停车是一个常见的事件，但有自由空间滚动和行人处于危险区域的的可能性与假定的坡度和距离相关。	--	驾驶员不在车内，假定可控性为C3，由于行人可能没有意识到危险或不能足够快速的反应。驾驶员仍然在车内，可控性取决于驾驶员状态（分心、匆忙等）和反应时间（与坡度和距离相关）。	--	参见D5.2的详细说明和指导

危害	功能	功能异常	整车层面	假设	危害的详细描	潜在的事故场景	ASIL（汽车安全完整性等级）的评估								备注
F5-4	提供防溜坡功能	无法关闭防溜坡功能。	--	与安全无关（S0）。	车辆处于静止，并且防溜坡功能启动，驾驶员想启动车辆。	车辆将继续处于静止状态。没有危害影响。	S0	车辆将继续处于静止状态，没有危害影响。	E4	车辆处于静止，并且防溜坡功能启动，驾驶员想启动车辆。	--		QM		
注：危害分析和风险评估后，需要针对各个危害定义安全目标，安全目标的定义可以考虑代表目标市场人员对风险控制能力的可控性度量结果。															

D.5 示例详述

本条提供了对表D.3的示例进行评估的具体步骤。

D.5.1 暴露概率等级的评估和计算

F5-1：提供防溜坡功能

针对本示例，可以解释对于暴露概率如何进行基于经验的评估。

F5-1d的危害场景示例：

详细场景：红灯时，车辆停在十字路口。信号灯变为绿色时，第一辆车启动并加速。侧面过来一辆车，这辆车的驾驶员预计第一辆车很快就会通过路口。此时，第一辆车的防溜坡功能非预期的启动，而两辆车之间的距离相当近。

评估/讨论：

第一步：讨论场景的相关方面，以提高对场景描述和相关参数定义的理解

假设当驱动轴有特定的最小速度（例如5km/ h）时，存在防止停车锁止被啮合的机械措施。所以故障必须发生在达到该速度之前。

在通常驾驶状况下，来自侧面车辆的驾驶员将识别到车辆正在通过路口，并将避免过快的进入十字路口。

第二步：对所需参数进行基于经验的评估

1. 假设加速时间：2s（直到达到5km/h）
2. 假设每个驾驶周期内遇到的十字路口次数：20次
3. 交叉路况中汽车以危险方式从侧面进入十字路口的相对数量：十分之一

第三步：计算场景持续时间

根据场景，暴露概率应基于持续时间（相对于运行时间）或基于频率（相对于驾驶次数）进行评估。为了进行定量的暴露度评估，对于这两种情况，必须指定一些基本数据。[1]基于这些数据，暴露度E的参数等级的上下限可以很容易地根据GB/T 34590.3-XXXX计算，如表D.4所示。

表D.4 暴露概率E等级的计算范围

	E1	E2	E3	E4
GB/T 34590 描述（持续时间）	无定义	<1%的平均运行时间	1%～10%的平均运行时间	>10%的平均运行时间
基于假设的运行时间[小时/年]	< 0.4 小时/年	0.4小时/年 < x <=4小时/年	4 小时/年 < x <= 40小时/年	> 40 小时/年
GB/T 34590描述（频率）	对大多数驾驶员而言，一年发生的频率小于一次	对大多数驾驶员而言，每年发生几次	对普通驾驶员而言，基本上每个月发生一次或多次	平均几乎发生在每次驾驶中
基于假设的驾驶次数[1/年]	< 1次/年	1次/年 < x < 10次/年	10次/年 < x < 100次/年	> 100次/年

对于给定的示例，暴露概率应基于持续时间评估，因故障可能立即导致危害[2]。所以计算如下：

•场景中平均持续时间的计算：每个驾驶周期4秒（根据上文中第二步的假设计算）。

•假设驾驶周期为1000次/年，可得出持续时间为4000秒/年，约1小时/年。

•因为它小于1%正常运行时间（400小时/年），故得出E2。

然而，这只是基于经验的预估，并不是完全由统计数据支持。特别是对结果影响较大的参数，应获得客户或现场的调查数据。

D.5.2 对暴露概率、严重度和可控性之间存在强相互依赖性的场景进行评估

F5-2：非预期的防溜坡功能关闭

---

1) 在本附录中，以下参数已被用作评估依据：平均运行时间：400小时/年。平均驾驶次数1000次/年：

2)要确定是基于持续时间还是频率进行暴露概率评估，在大多数情况下，适用以下简单规则：故障发生时，如果故障直接起作用（故障触发危害），可基于持续时间（多长时间）评估。如果故障潜伏直到场景出现（场景触发危害），可基于频率评估（多少频次）。

对于像示例F5-2这样的功能异常表现，必须分析暴露概率、严重度和可控性之间的强相互依赖性，以便对一组场景做出适当的风险评估。具体如何去做，下面将给出一些附加指导。

F5-2的危害场景示例：

车辆停在斜坡（发动机熄火），有足够的自由空间滑动（以达到危害的速度）。驾驶员已经离开了车辆，当失效发生时，行人处于危险区域（下坡）。

评估/讨论：

第1步：讨论场景的相关方面，以提高对场景描述和相关参数定义的理解

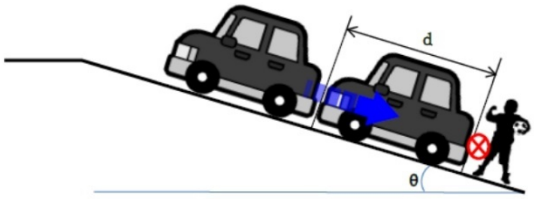


图 D.1 F5-2 场景图解

条件假设：

在故障发生之前，本车处于静止状态，开启防溜车功能。因驾驶员离开车辆，故避免危害是不可能的。由于没有关于行人避免危害行动的预估参考，可假设定义为C3。

参数：

坡度（影响车辆的加速度）

车辆和行人的距离

第2步：相关参数的模拟计算

通过按坡度得到的加速度以及车辆与行人间距离（对应于持续时间）作为参数来计算碰撞速度。再结合E和S判断（限制值），可以用于为所有相关场景导出ASIL等级。

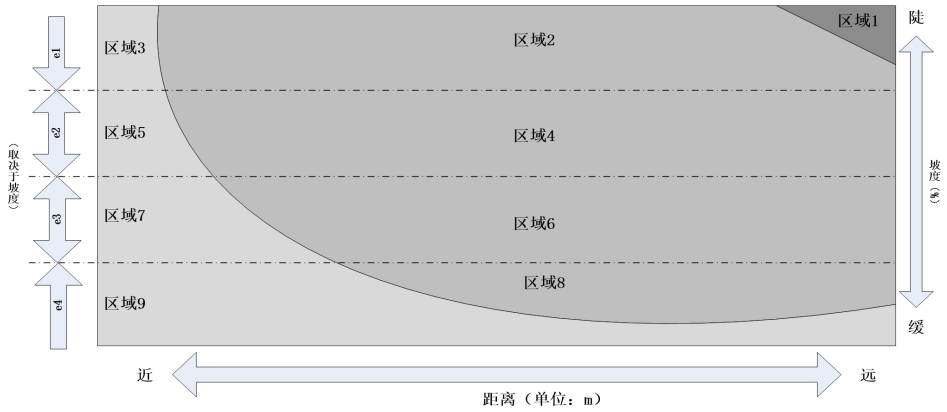


图 D.2 F5-2 场景严重度示意图

第3步：典型场景和ASIL等级

整体场景的可控性等级为C3，因为驾驶员离开了车辆，并且对于近距离事件，行人的反应是无法假设的。（因为没有关于行人何时能注意到移动车辆的数据，故行人的避免危害的行动不可知）。

严重度等级的确定基于以下模拟：

纵向：坡度对应的加速度数值（g）

侧向：车辆和行人之间的距离对应的加速度时间

→对于后方碰撞行人来讲，碰撞速度作为主要的S准则。

- （深灰色区域）→ S3区域
- （灰色区域）→ S2区域

•（浅灰色区域）→ S1区域

暴露概率等级的确定需要一个综合的判断，即根据作为一定等级概率e（θ）的暴露条件和行人处于危险区域的持续时间e（d）。例如根据e3（θ）和e3（d）的组合，区域6的整体暴露概率被评为E2。

最后，根据HARA评估表，可以选择具有最高ASIL的示例作为“典型场景”。

此外，还必须分析其它场景以找出何种情况导致最高的ASIL。HARA宜包含以下方面：

•驾驶员仍在车内的场景（影响E和C）；

•驾驶员分心或匆忙离开车辆（影响E和C）；

•与侧面车辆碰撞（影响S、E和C）。

在适当的情况下，可以使用如上所示的类似分析方法来阐述一致的典型场景。

D.5.3 关于非预期加速（稳定）场景的评估

F3-1a：提供的驱动扭矩大于需求

提供的驱动扭矩大于需求的功能异常表现可能导致车辆的非预期加速。为了根据这一危害进行适当的风险评估，必须考虑以下几个方面。

用于评估的最主要场景，一种情况是车辆跟随另一车辆，可能发生追尾碰撞，另一种情况是车辆以非常低的速度行驶，行人处于车辆前方的危险区域。如何评估具体系统和车辆的场景，下面提供了一些附加指导：

场景1：行驶在另一车辆后面

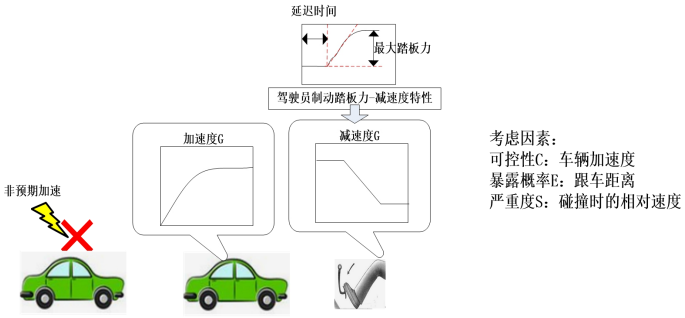


图 D.3 场景 F3-1a 图解

为了正确评估风险，必须分析图D.3所示的几个参数：

•车辆加速度的变化；

•来自于驾驶员以一定的力踩制动踏板的有效减速度；

•两辆车之间不同距离的暴露概率；

•不同类型车辆的暴露概率，假设车辆类型不同会导致不同的严重度（例如：如果另一车辆是重型卡车，碰撞时的相对速度较高，但跟随卡车的概率低于跟随普通乘用车的概率）。

场景2：低速行驶，且行人处在危险区域：

这种场景适用于车辆低速驾驶（例如1档），且行人处在汽车行驶方向。常见的例子是十字路口或停车场。

为了适当地评估风险，一种方法是将重点放在可能造成致命伤害（例如：辗轧）的最严苛场景，且通过控制车辆来避免这种特定伤害的机会很小。当一些边界条件成立时就会发生这种情况：

•驾驶员很容易无法控制的驾驶操作情况；

•行人正处在车前方的危险区域；

•车辆和行人之间没有其他障碍物可防止碰撞；

•行人处在可能被辗轧的位置。

注：最后一个条件取决于车辆的具体设计，因为在相同的情况下，某些车辆比其它车辆更可能发生辗轧。相关车辆具体设计方面的例子有：离地间隙、正面轮廓、被动行人保护措施。

暴露概率评估指导：

驾驶周期的很大比例包括行人所在区域（例如：十字路口、停车场）。不过，据评估，花费在这些地方的驾驶时间只占一定的比例，且行人并不总是在汽车前面的危险区域。

由于重点在于辗轧场景，所以概率在一定程度上又进一步降低。然而，目前还没有确定的数据可将暴露概率的等级视为所有车辆的普遍结果。

附 录 E
（资料性）
悬架控制功能的危害分析和风险评估示例

E.1 简介

本附录提供了悬架控制功能的危害分析和风险评估的示例。E.3 提供了一个HAZOP分析，来识别少数悬挂控制功能的功能异常表现。E.4提供了部分悬架控制的功能异常，及其导致的整车层面的危害和相关的ASIL等级示例。必须指出，本附录作为悬架功能危害分析和风险评估的指导，仅仅分析了少数悬架控制功能所涉及的部分危害，不能代表所有悬架控制功能的完整危害分析和风险评估。

注：本资料性附录包含了所选危害事件的ASIL等级示例。ASIL等级的确定，由相关方协商确定。

E.2 相关项定义：功能概念概述

悬架控制功能的主要作用是增强车辆在转弯时的操纵特性，并通过对路面噪音和震动的阻尼作用，改善车辆行驶的舒适性。本示例中分析的范围包含四种悬架控制功能：阻尼控制、水平控制、刚度控制和侧倾控制。这些控制功能在被动、半主动和主动控制悬架中不尽相同。在半主动和主动控制功能中，电子传感器和控制器会用于控制悬架的阻尼器、空气弹簧、吸振器、横向稳定杆以及其他悬架设备。

E.3 危害分析

表E.1展示了通过HAZOP分析识别出的少数悬架控制功能的功能异常表现。许多悬架控制功能的故障会对应一个以上的整车层面的危害，E.4,表E.2中列举了整车层面的危害示例。

表E.1 悬架控制功能HAZOP分析

功能	引导词					
	功能丧失	在有需求时，提供错误的功能			非预期的功能（在无需求时，提供功能）	输出卡滞在固定值上（功能不能按照需求更新）
		错误的功能（多于预期）	错误的功能（少于预期）	错误的功能（方向相反）		
阻尼控制（控制阻尼系数）	丧失阻尼控制	过度的阻尼控制	不足的阻尼控制	相反的阻尼控制（在需求的反方向施加了阻尼）	非预期的阻尼控制（自动阻尼）	阻尼无法调整
水平控制（控制每个车轮的水平位置）	丧失水平控制	过度的水平控制	不足的水平控制	相反的水平控制	非预期的水平控制	水平位置无法调整
刚度控制（控制悬架刚度）	丧失刚度控制	过度的刚度控制	不足的刚度控制	相反的刚度控制	非预期的刚度控制	刚度无法调整
侧倾控制（改进车辆侧倾稳定性）	丧失侧倾控制	过度的侧倾控制	不足的侧倾控制	相反的侧倾控制	非预期的侧倾控制	侧倾控制锁止

E.4 危害分析和风险评估

表E.2列举了少数悬架控制功能的危害分析与风险评估的示例。

表E.2 悬架控制功能危害分析和风险评估示例

危害编号	功能	功能异常表现	整车层面的危险	假设	危害的详细描述	潜在的事故场景 -考虑最严苛场景	ASIL（汽车安全完整性等级）的评估	备注
悬架危害1	阻尼控制	非预期或者不正确的阻尼控制	非预期的车辆运动（侧向、纵向、垂向）	半主动悬架系统：控制阻尼器的阻尼系数。在阻尼控制的各个状态下，车辆都可能失稳。	在某些行驶工况下，阻尼控制功能的异常会导致潜在的丧失对轮胎的纵向以及或者侧向牵引力。这可能导致非预期的降低车辆稳定性或者增加制动距离。	行驶场景为急转弯或者变道（0.3g~0.5g的中等侧向加速度），同时路面的扰动达到非簧载质量的垂向共振频率。	根据车辆的不同，可能的ASIL等级范围：QM~A	各个悬架功能的ASIL分级取决于车辆、功能的权限和设计。如果在阻尼控制功能的权限内，所有可能的功能异常状态都不会导致车辆失稳，那么该危害不适用。
悬架危害2	水平控制	对一个或者多个车轮不正确或者非预期的水平控制	非预期的车辆运动（侧向、纵向、垂向）	对每个车轮的独立的主动水平控制	在一个或多个轮子上的非预期或不正确的水平控制会影响车辆的重心，或导致车轮上的力分布不正确。	最严苛场景为急转弯或者连续变道（0.3g~0.5g的中等侧向加速度），此时水平控制功能异常可能引起车辆横摆力矩或者侧倾力矩。	根据车辆的不同，可能的ASIL等级范围：QM~C	各个悬架功能的ASIL分级取决于车辆、功能的权限和设计。如果在水平控制功能的权限内，所有可能的功能异常状态都不会导致车辆失稳，那么该危害不适用。
悬架危害3	刚度控制	不正确或非预期的刚度控制作用在一个或者多个车轮	非预期的车辆运动（侧向、纵向、垂向）	对每个车轮的独立的主动刚度控制	在某些行驶工况下，刚度控制功能的功能异常会导致潜在的纵向或者侧向轮胎牵引力丧失。这可能导致非预期的降低车辆稳定性或者增加制动距离。	最严苛场景为急转弯或者连续变道过程中（0.3g~0.5g的中等侧向加速度）对角车轮刚度控制的分配不均匀。此时刚度控制功能异常可能引起车辆横摆力矩或侧倾力矩。	根据车辆的不同，可能的ASIL等级范围：QM~B	各个悬架功能的ASIL分级取决于车辆、功能的权限和设计。如果在刚度控制功能的权限内，所有可能的功能异常状态都不会导致车辆失稳，那么该危害不适用。
悬架危害4	侧倾控制	非预期或者不正确的激活侧倾控制	非预期的车辆运动（侧向、纵向、垂向）	主动侧倾控制独立的控制每个车轴的侧倾力矩	在某些行驶工况下，侧倾控制功能的功能异常会导致潜在的丧失对轮胎的纵向以及或者侧向牵引力。这可能导致非预期的降低车辆稳定性或者增加制动距离。	在侧向加速度较大的行驶工况下，非预期的侧倾力矩可能导致车辆失稳。	根据车辆的不同，可能的ASIL等级范围：QM~B	各个悬架功能的ASIL分级取决于车辆、功能的权限和设计。如果在主动侧倾控制功能的权限内，所有可能的功能异常状态都不会导致车辆失稳，那么该危害不适用。
注：危害分析和风险评估后，需要针对各个危害定义安全目标，安全目标的定义可以考虑代表目标市场人员对风险控制能力的可控性度量结果。								

E.5 其他注意事项

悬架控制功能在被动、半主动和主动控制悬架中不尽相同。当进行悬架控制功能的危害分析和风险评估时，需要考虑控制功能的类型和权限对车辆控制的影响，并结合车辆的总体设计，从而评估安全目标的ASIL等级，最终的ASIL等级取决于具体车辆。

附 录 F
（资料性）
制动和驻车制动功能危害分析和风险评估示例

F.1 总则

本附录提供了使用危害分析和风险评估来确定ASIL等级，并满足GB/T 34590要求的示例、指导和论据。仅考虑了制动和驻车制动功能中最相关的功能异常表现和整车层面的危害。本附录不能代表制动及驻车制动功能完整的危害分析和风险评估。这些示例对定义任何特定的车辆系统的最低或最高的ASIL等级不是必要的。本附录的目的是为评估特定的整车危害提供指南。每个危害的讨论结果采用下面三种方法中的一种方法来呈现：

a) ASIL 等级和 ASIL 等级的范围；
b) 无认同的 ASIL 等级，但 ASIL 等级的上限已确定；
c) 无认同的 ASIL 等级，但为用于确定 ASIL 等级的参数取值提供指南。

即使是已发布的达成一致的ASIL等级，仍有可能使用了不同的ASIL等级定义过程以及不同的S、E、C值。对于特定应用的危害分析和风险评估，还需评估额外的场景，以发现对于一个特定的安全目标，究竟是哪个场景给出了最高的ASIL。

注：本资料性附录包含了所选危害事件的ASIL等级示例。ASIL等级的确定，由相关方协商确定。

F.2 相关项定义：功能概念概述

F.2.1 制动功能

本附录所涉及制动的主要功能的目的是:

——基于驾驶员经由制动踏板的输入或整车其他系统（例如：驾驶员辅助系统）的输入，为整车提供减速；

——在接近车辆动态的物理极限的场景中通过执行车轮制动（例如，通过稳定性控制、防抱死系统、电子制动力分配等功能），为整车提供稳定性。

F.2.1.1 稳定性控制

稳定性控制功能是一项安全辅助或安全增强型功能,其主要功能是辅助驾驶员保持对车辆的可控性。稳定性控制利用车上的传感器来判断驾驶员的输入意图是否与车辆的方向保持一致。如果稳定性控制监测到不一致，它可通过控制制动功能或节气门功能来帮助纠正不一致。

F.2.1.2 防抱死系统（ABS）

ABS是一项安全辅助或安全增强型功能，其主要功能是防止车轮锁止，以帮助避免不受控的打滑或帮助减少制动距离。ABS监控每一个车轮的速度，如检测到某个车轮的转动速度比其他轮胎的要更慢或更快，就以一种特定的节奏来控制制动。

F.2.1.3 电子制动力分配（EBD）

EBD的主要功能是优化基础制动系统的效率和稳定性。它通过调整后轮的制动压力接近至理想制动力分配来防止后轮的过度制动，由此可在不考虑车辆载荷的情况下对后轴制动进行优化。

F.2.2 驻车制动功能

驻车制动的主要功能是保持车辆处于静止状态。本附录中涉及的驻车制动子功能包括驻车制动激活或驻车制动结合，以及驻车制动释放，两者都是基于驾驶员的请求。

F.3 HAZOP 分析

F.3.1 主制动功能

表F.1给出了为识别制动功能的功能异常表现而做的HAZOP分析。表F.2给出了制动功能异常表现与整车层面危害的映射。

表F.1 制动功能的HAZAOP分析

功能	引导词					
	功能丧失	在有需求时，提供错误的功能			非预期的功能（在无需求时，提供功能）	输出卡滞在固定值上（功能不能按照需求更新）
		错误的功能（多于预期）	错误的功能（少于预期）	错误的功能（方向相反）		
减速	丧失制动	过度制动	制动不足	N/A	非预期制动	制动锁死

表F.2 制动功能的功能异常表现映射到整车层面危害的示例

功能异常表现	整车层面危害
非预期制动	非预期的车辆纵向减速
制动抱死	
过度制动	
制动不足	非预期的车辆减速能力下降
丧失制动	
非预期制动	非预期的车辆侧向运动
制动抱死	
过度制动	
非预期的丧失稳定性控制，防抱死（ABS）控制或者电子制动力分配（EBD）控制功能	非预期的丧失车辆制动控制功能

F.3.2 驻车制动主要功能

表F.3给出了为识别驻车制动功能的功能异常表现而做的HAZOP分析。表F.4给出了驻车制动功能的功能异常表现与整车层面危害的映射。

表F,3 驻车制动功能的HAZOP分析

功能	引导词					
	功能丧失	在有需求时，提供错误的功能			非预期的功能（在无需求时，提供功能）	输出卡滞在固定值上（功能不能按照需求更新）
		错误的功能（多于预期）	错误的功能（少于预期）	错误的功能（方向相反）		
驻车制动结合	丧失驻车制动结合的能力	N/A	驻车制动力不足	N/A	非预期的驻车制动结合	丧失驻车制动释放的能力
驻车释放	丧失驻车制动释放的能力	N/A	驻车制动不能完全释放	N/A	非预期的驻车制动释放	N/A

表F.4 驻车制动的功能异常表现映射到整车层面危害的示例

功能异常表现	整车层面危害
非预期的驻车制动结合	非预期的车辆侧向运动
	非预期的车辆纵向减速
非预期的驻车制动释放	非预期的车辆纵向运动
驻车制动失效	
驻车制动力不足	
驻车制动不能释放	非预期的丧失车辆纵向运动功能
驻车制动不能完全释放	

F.4 危害分析和风险评估

F.4.1 制动功能的危害分析和风险评估

表F.5给出了制动功能危害分析和风险评估的示例。

表 F.5 制动功能的 HARA 分析示例

危害编号	功能	功能异常表现	整车层面的危害	假设	危害的详细描述	潜在的事故场景－考虑最严苛场景	ASIL（汽车安全完整性等级）的评估							备注
							S	理由	E	理由	C	理由	ASIL	
制动危害1	减速	非预期制动	非预期的车辆纵向减速	无车轮抱死	制动系统在没有制动请求的情况下提供制动	若跟随车辆距离太近无法停车，则会引发追尾	涉及的参数可能包括车速和时间间隔（从两车车速导出的特征）、因功能异常引起的减速度数值、涉及车辆的质量比、安全装置和乘员约束装置、反应时间以及跟随车辆的减速度数值和变化率(驾驶员能力)。 其他参数也可以考虑。							见F.1（iii）
制动危害2	减速	制动不足	非预期的车辆减速度降低	无	制动系统提供的制动少于实际需求	因制动不足导致的潜在碰撞	取决于制动力降低的程度						QM~D	见F.1（ii）
制动危害3	减速	非预期制动	非预期的车辆侧向运动	车轮锁止，影响整车稳定性	制动系统在没有制动请求的情况下提供制动	潜在的车辆偏离车道与其他车辆、行人或者物体发生碰撞	S3	最苛刻场景的潜在事故可导致S3级别的严重度	E4	每天在高附着力路面驾驶	C3	难以控制	D	见F.1（ii）
制动危害4	拖曳力控制	非预期激活拖曳力控制	非预期的车辆加速	无			危害项已被驱动系统功能的附录覆盖,见D.4.2（危害编号F3)。							
制动危害5	牵引力控制	非预期激活牵引力控制	非预期失去车辆加速	无			危害项已被驱动系统功能的附录覆盖,见D4.2（危害编号F3)。							
制动危害6	稳定性控制	非预期丧失制动横摆功能	非预期丧失车辆制动横摆稳定性控制	驾驶员需要高的侧向加速度G	稳定性控制功能不可用		S3	最严苛场景的潜在事故可导致S3级别的严重度	E1	稀有案例	C3	难以控制	A	没有警告提示
制动危害7	防抱死系统（ABS）	非预期丧失ABS功能	非预期丧失车辆ABS功能	驾驶员需要在低附着力路面上减速	防抱死系统（ABS）不可用		S3	最严苛场景的潜在事故可导致S3级别的严重度	E1	稀有案例	C3	难以控制	A	没有警告提示
制动危害8	电子制动力分配	非预期丧失电子制动力分配功能	非预期丧失车辆电子制动力分配(EBD)功能	驾驶员需要大的减速度	电子制动力分配功能（EBD）不可用		S3	最严苛场景的潜在事故可导致S3级别的严重度	E1~E3	取决于车辆（制动设计和整车概念）	C3	难以控制	QM~C	见F.1（ii）
注：危害分析和风险评估后，需要针对各个危害定义安全目标，安全目标的定义可以考虑代表目标市场人员对风险控制能力的可控性度量结果。														

F.4.2　驻车制动功能的危害分析和风险评估

表F.6给出了驻车制动功能的危害分析与风险评估的示例。

表F.6 驻车制动功能的危害分析和风险评估示例

危害编号	功能	功能异常表现	整车层面的危害	假设	危害的详细描述	潜在的事故场景－考虑最严苛场景	ASIL（汽车安全完整性等级）的评估							备注
							S	理由	E	理由	C	理由	ASIL	
驻车制动危害1	驻车制动	后驻车制动的非预期结合	非预期的车辆侧向移动	没有	后驻车制动非预期的结合	当车辆处于运行状态中激活驻车制动会导致车辆侧向移动，并与其他车辆、行人或物体发生碰撞。	S3	最严苛场景的潜在事故可导致S3级别的严重度	E4	由于可以发生在任何类型的道路上，故而平均运行时间超过10%以上，见GB/T 34590.3-XXXX第3部分，表B.2	C3	少于全部驾驶员和交通参与者的90%的人能够避免非预期侧向移动的危害。	D	最严苛场景
驻车制动危害2	驻车制动	后驻车制动的非预期结合	非预期的车辆纵向减速	无	后驻车制动非预期的结合	当车辆处于运行状态中激活驻车制动，如果跟随车辆距离太近而无法停车，会导致追尾	取决于车辆的动力学考虑，如制动设计和车辆概念。						QM~C	见制动危害1，用于额外考虑。
驻车制动危害3	驻车制动	后驻车制动非预期释放	非预期的车辆纵向移动	手动变速箱;车辆变速箱不在驻车档	后驻车制动非预期的释放	潜在的最严苛场景是：当驻车制动释放时，司机不在车内，引擎还在运行。	相关项已经被驱动系统功能的附录覆盖，见D.5.2 和D4.2（危害序号F5-2）。							
驻车制动危害4	驻车制动	后驻车制动失效无法结合	非预期的车辆纵向移动	无	当需要时后驻车制动失效	驻车制动失效导致车辆非预期的纵向移动，并与其他车辆、行人或物体发生潜在碰撞.	相关项已经被驱动系统功能的附录覆盖，见D.5.2 和D4.2（危害序号F5-3)。							
驻车制动危害5	驻车制动	后驻车制动未能释放	非预期的失去车辆纵向移动	无	当请求时后驻车制动未能释放	辆驻车不能移动，因此无危害	相关项已经被驱动系统功能的附录覆盖，见D.4.2（危害序号　F5-4)。							
注：危害分析和风险评估后，需要针对各个危害定义安全目标，安全目标的定义可以考虑代表目标市场人员对风险控制能力的可控性度量结果。														

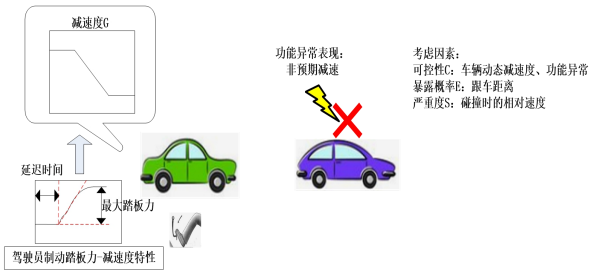
F.5 示例的说明和细节描述

在附录的这部分中，给出了关于如何对表F.4中的示例进行评估的一些更详细的背景信息。

F.5.1 与非预期车辆纵向减速相关场景的评估（应用于制动危害1和驻车制动危害2）。

功能异常表现被描述为在没有驾驶员意图的情况下提供更多的制动扭矩，从而导致车辆的非预期减速。依据这种危害对风险进行适当的评估，可以考虑几个方面。评估中最重要的场景通常是出现故障的车辆后面跟随着另一辆车，可能发生追尾碰撞的情况。下面的段落提供了关于如何针对自身系统和车辆对这种情景进行评估的一些额外指导。

场景：在其他车辆后面行驶



图F.1 危害场景图解

为了恰当的评估该风险，图F.1中给出的几个参数可包括在分析中：

——车辆动态减速度、功能异常；

——来自于（后车）驾驶员的反应，以一定的力和速率踩下制动踏板而产生的有效减速；

——不同速度的两辆车之间的车间距的暴露概率；

——不同类型的车辆的暴露概率，如果这会导致不同的严重度（例如:如果另一辆车是重型卡车，碰撞时的△V 速度变化量比较高，但是一辆卡车跟在后面的可能性要比一辆常规乘用车跟在后面的概率低）。

基于车辆系统的动态减速度和潜在的功能异常，可能的组合（例如:跟随距离、碰撞速度、反应时间等）在分析中起重要作用，并可能导出一个ASIL等级的范围。需要额外的研究去恰当的评估整车环境下的功能异常表现。

参 考 文 献

[1] Ministry of Defence, “Defence Standard 00-58 HAZOP Studies on Items Containing Programmable Electronics”, Issue 2, 19 May 2000

[2] Code of Practice for the design and evaluation of ADAS, EU Project RESPONSE 3: Oct. 2006

[3]http://www.acea.be/publications/article/code-of-practice-for-the-design-and-evaluation-of-adas

[4] GIDAS, http://www.vufo.de/forschung-und-entwicklung/gidas/?L=1

[5] ITARDA, http://www.itarda.or.jp/english/e_outline1.php

[6] NASS/CDS, http://www.nhtsa.gov/NASS